

Michigan Cyber Initiative News

January 2013, Issue 11

Articles of Interest

Michigan's Tech Trio Ready to Prove the Power of Good IT

Michigan Gov. Rick Snyder knew he had a technology problem the first time he visited his state Capitol office. — To read this article, click [here](#).

Smartphone Apps can Compromise Kids' Data, FTC says

Parents are finding it more difficult to keep their children's private personal data from being collected by mobile phone apps, according to a new report. — To read this article, click [here](#).

911 Emergency Texting Coming in 2014 from 'Big Four' Carriers

The Federal Communications Commission says the nation's four largest wireless carriers have agreed to relay text messages to text-enabled 911 call centers by May 2014. — To read this article, click [here](#).

Nationwide Insurance Data Breach Affects 1.1 Million People

Nationwide Mutual Insurance Company fell victim to hackers in October, affecting an estimated 1.1 million individuals. — To read this article, click [here](#).

Analysis of U.S. Breach Data Finds Reasons for Concern

The healthcare industry has made little progress in reducing the number of breaches with troubling statistics seen from the same types of organizations, breaches and locations. — To read this article, click [here](#).

Did you Know?

There is a timeline of data breaches you can view by going to <http://www.privacyrights.org/data-breach>.

Some of the information provided includes the type of breach, where it happened and some details on how it happened.

You can filter searches by organization type, year and breach type.

Protect your Identity while Protecting Trees

Below are some tips to protect your identity that will also help save trees.

- Instead of printing a document and filing it away, use a secured storage device. Be sure to put it in a safe place and have a back-up.
- Choose to do online banking and billing. Verify that the site you are using is secure.
- Use email to share a document. Be sure to follow the guidelines around the information you are emailing and encrypt all digital correspondence. You may even want to include a disclaimer at the bottom of your email.
- Redact information from the digital file rather than a printed document. This should prove to be quicker and easier.

Update: 2013 Cyber Summit

All good things must come to an end, and the 2012 Michigan Cyber Awareness Breakfast Series has come to an end.

However, the good news is that we are in the process of planning a Cyber Summit for 2013. Once we finalize the location and date we will be sure to let you know.

For all attendees of the cyber breakfast, you should have received a survey via email. Be sure to fill it out and send it back. Your responses are appreciated and will help us with future events.

2012 Review: Most Significant Data Breaches

By: Dan Lohrmann

What were the top government data breaches in the USA in 2012 (so far)? It appears that this year will be remembered more for state and local breach headlines than for federal government breaches.

I'm starting off this blog with highlights from one of those "scary headline" articles that government technology leaders want their organizations to avoid. And yet, there is an ominous sense across the nation right now amongst security professionals. Most Chief Information Security Officers (CISOs) understand that there are more breaches to come in 2013. To some extent, the sentiment is: "I could be next."

A shout-out goes to Rock Rakowski, one of our Michigan cybersecurity managers, who sent me an excellent article which addressed this question and even listed lessons learned' from each breach. The [article was written by Ericka Chickowski](#) for *Dark Reading*. Here's the abbreviated first five on the list, but I urge you to read her entire piece, including the recommendations:

- 1) South Carolina – 3.3 million unencrypted bank account numbers and 3.8 million tax returns...
- 2) California Department of Social Services - Sensitive payroll information about approximately 700,000 individuals...
- 3) Utah Department of Health - The health information and PII of more than 780,000 Utah citizens...
- 4) California Department of Child Support Services - lost more than 800,000 sensitive health and financial records...
- 5) United States Bureau of Justice Statistics - Anon-ymous embarrassed the United States Bureau of Justice Statistics (BJS) when it leaked 1.7 GB of sensitive data...

So What Other USA Breaches Have We Seen This Year?

This [Network World slide show](#) listed the top breaches

through June 2012. Naming 13.73 million records within 189 major breaches, while the government breaches are mentioned, the top two breaches named were:

1) *"New York State Electric & Gas Co. - Number of records exposed: 1.8 million files that contained customer Social Security numbers, dates of birth and bank account number, due to unauthorized access by a contractor."*

2) *Global Payments, Inc. - Atlanta, Ga. - No. of records exposed: 1.5 million payment-card numbers, plus in June the company disclosed its investigation is also turning up potentially hacked servers with names of merchant applicants."*

Wrap-Up

In conclusion, 2012 (minus December) has already been one of the top years for data breaches, and certainly the most significant year for government data breaches at the state and local level. The breach trends do not look good going into 2013.

Of course, the presidential election news in 2012 and the current [fiscal cliff headlines](#) continue to move cybersecurity stories and breach headlines into a lower priority category for citizen engagement. True, these breach stories get some front-page attention, but the news-talk radio focus is simply not there yet.

However, I believe that sooner or later these issues will be seen as a national crisis that needs to be addressed with an additional level of focus. The country is also ready for a change in the way we communicate credit card, social security, health records and other sensitive information. Passing this data around openly plastic cards, telephones and unencrypted emails is simply too 20th century.

To read the full article, click [here](#).

Excerpted by permission from Lohrmann on Cybersecurity, www.govtech.com, December 2, 2012.



Email: MI-Cyber-Initiative@michigan.gov
Website: www.michigan.gov/cybersecurity

Subscribe to our distribution list by emailing the word "Subscribe" to MI-Cyber-Initiative@michigan.gov